

Wireless Information Surveillance via Proactive Eavesdropping with Spoofing Relay

Yong Zeng* and Rui Zhang

Abstract—Wireless information surveillance, by which suspicious wireless communications are closely monitored by legitimate agencies, is an integral part of national security. To enhance the information surveillance capability, we propose in this paper a new proactive eavesdropping approach via a spoofing relay, where the legitimate monitor operates in a full-duplex manner with simultaneous eavesdropping and spoofing relaying to vary the source transmission rate in favor of the eavesdropping performance. To this end, a power splitting receiver is proposed, where the signal received at each antenna of the legitimate monitor is split into two parts for information eavesdropping and spoofing relaying, respectively. We formulate an optimization problem to maximize the achievable eavesdropping rate by jointly optimizing the power splitting ratios and relay beamforming matrix at the multi-antenna monitor. Depending on the suspicious and eavesdropping channel conditions, the optimal solution corresponds to three possible spoofing relay strategies, namely *constructive relaying*, *jamming*, and *simultaneous jamming and destructive relaying*. Numerical results show that the proposed technique significantly improves the eavesdropping rate of the legitimate monitor as compared to the existing passive eavesdropping and jamming-based eavesdropping schemes.

Index Terms—Wireless information surveillance, proactive eavesdropping, spoofing relay, power splitting, beamforming, jamming.

I. INTRODUCTION

The great success of wireless communication technology has drastically improved our life during the past few decades. By providing high-speed wireless connectivity essentially anywhere, anytime, and between any pair of devices, contemporary wireless communication systems not only make our daily life increasingly more convenient, but also provide numerous new opportunities for applications and innovations in almost all fields, such as education, business, industry, etc. However, the ubiquitous accessibility of wireless communication systems also makes them more vulnerable to be misused by malicious users to commit crimes, jeopardize the public safety, and invade the privacy of others, etc. Therefore, it becomes increasingly important for the legitimate parties, such as the government agencies, to implement effective information surveillance measures to monitor any suspicious

communication for various purposes such as intelligence gathering, terrorism/crime prevention and investigation, etc.

From an engineering design perspective, devising efficient schemes for wireless information surveillance calls for a paradigm shift from that for conventional wireless security [1], [2]. In wireless security, the eavesdroppers are treated as adversaries, whose eavesdropping potential should be minimized. Various wireless security mechanisms, both in physical layer [3] and across upper layers of communication system protocols design [4], have been proposed to prevent or minimize the information leakage to the unintended eavesdroppers. In particular, under the classic wiretap channel setup [5], significant efforts have been devoted to characterizing the *secrecy capacity* [6]–[8], defined as the maximum transmission rate at which the message can be reliably decoded at the legitimate receiver without leaking any useful information to eavesdropping receivers. For wireless surveillance, however, the monitor is regarded as a legitimate eavesdropper, whose eavesdropping rate over any suspicious channel should be maximized to effectively intercept the transmitted information over the air.

One straightforward approach for wireless information surveillance is passive eavesdropping, where the legitimate monitor only listens to the wireless channels of any suspicious users to decode their transmitted messages. However, this approach is effective only when the eavesdropping channel from the source to the legitimate monitor is better than the suspicious channel to the destination, so that the information sent by the suspicious source can be reliably decoded at the legitimate monitor. Yet this does not hold in practice if the legitimate monitor is located further away from the suspicious source compared to the suspicious destination. To overcome this limitation, a proactive eavesdropping scheme via cognitive jamming technique is proposed in [1], [2], where the legitimate monitor sends noise-like jamming signals to intentionally degrade the suspicious link, so as to induce the suspicious source to reduce transmission rate to be decodable at the legitimate monitor receiver. However, given the limited power budget for jamming, the eavesdropping performance cannot be improved if the suspicious channel capacity is higher than that of the eavesdropping channel even with the maximum-power jamming. Furthermore, there are also scenarios when it is desirable for the legitimate monitor to spoof the suspicious source to increase its transmission rate to achieve higher eavesdropping rate. In such cases, jamming is not effective and more intelligent strategies need to be devised for proactive eavesdropping.

To further enhance the information surveillance capability

Y. Zeng (corresponding author) is with the Department of Electrical and Computer Engineering, National University of Singapore (e-mail: elezeng@nus.edu.sg).

R. Zhang is with the Department of Electrical and Computer Engineering, National University of Singapore (e-mail: elezhang@nus.edu.sg). He is also with the Institute for Infocomm Research, A*STAR, Singapore.

This work has been presented in part at the 41th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 20-25 March 2016, Shanghai, China.

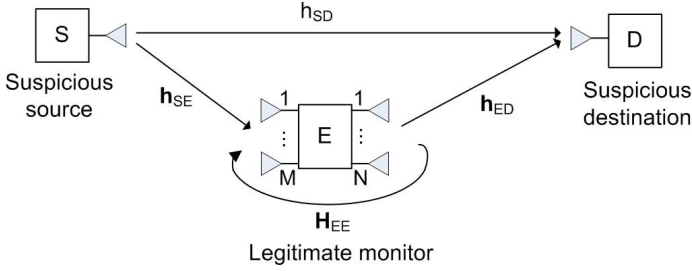


Fig. 1: Wireless information surveillance via a multi-antenna legitimate monitor.

of legitimate monitors, we propose in this paper a new proactive eavesdropping approach via a so-called *spoofing relay* technique. Specifically, besides information eavesdropping, the legitimate monitor also acts concurrently as a relay to send spoofing signals to the suspicious destination and thereby induce the source to vary the transmission rate in favor of the eavesdropping performance. The underlying assumption is that adaptive rate transmission is adopted at the suspicious source based on the effective channel condition at the destination. Under this setup, if the eavesdropping link (from the source to the legitimate monitor) is stronger than the suspicious link (from the source to the destination), the legitimate monitor will enhance the effective channel of the suspicious link by forwarding a constructive source signal to the suspicious destination, which leads to higher transmission rate by the suspicious source, and thus higher eavesdropping rate. On the other hand, if the eavesdropping link is weaker than the suspicious link, the legitimate monitor will degrade the effective channel of the suspicious link via forwarding a destructive source signal and/or a noise-like jamming signal to the suspicious destination, so as to spoof the suspicious source to reduce its transmission rate to a level decodable by the eavesdropping monitor. Note that the proposed spoofing relay technique is quite general since it is applicable regardless of whether the eavesdropping link is stronger or weaker than the suspicious link. Furthermore, it includes the existing passive and jamming-based eavesdropping [1], [2] as special cases, and thus is expected to outperform these two benchmark schemes. Intuitively, the proposed spoofing relay scheme is strictly beneficial when either the eavesdropping link is stronger than the suspicious link (so that constructive relaying improves the eavesdropping rate), or when the eavesdropping link is too weak such that jamming alone is insufficient (so destructive relaying is needed), as will be verified later in this paper by numerical results. The main contributions of this paper are summarized as follows.

- First, we model the system architecture for wireless information surveillance via a legitimate multi-antenna monitor, as shown in Fig. 1. A power splitting receiver¹ is proposed to split the received signal at each receiving antenna of the legitimate monitor into two parts, one

¹Notice that power splitting technique has also been used for separating the received signal for information decoding and energy harvesting in simultaneous wireless information and power transfer (SWIPT) systems [9], [10].

for information eavesdropping and the other for spoofing relaying. An optimization problem is then formulated to maximize the eavesdropping rate by the legitimate monitor via jointly optimizing the power splitting ratios for all of its receiving antennas and the relay beamforming/precoding matrix for the transmitting antennas.

- Next, we derive the optimal solution to the formulated problem by first solving two key sub-problems, which respectively find the maximum and minimum effective signal-to-noise ratio (SNR) at the suspicious link receiver by optimizing the relay precoding matrix at the legitimate monitor transmitter with fixed receiver power splitting ratios. Based on the obtained solutions, we further show that uniform power splitting, i.e., all receiving antennas at the legitimate monitor use the same power splitting ratio, is optimal for maximizing the eavesdropping rate with spoofing relaying, which thus leads to an efficient solution for the optimal power splitting ratios. Finally, the problem is solved with three possible relay strategies at the legitimate monitor, namely *constructive relaying*, *jamming*, and *simultaneous jamming and destructive relaying*, which are applied when the eavesdropping channel is better, weaker, and severely weaker than the suspicious channel, respectively.
- At last, numerical results are provided, which show that the eavesdropping rate achievable by the proposed spoofing relay scheme is significantly higher than that of the two benchmark schemes, namely passive eavesdropping and jamming-based proactive eavesdropping [1], [2].

It is worth pointing out that under the classic physical-layer security framework, secure communication for wireless relay channels has been studied in various setups. Depending on the role of the relay node, such existing works can be loosely classified into three categories: (i) *trusted relay* that helps the source transmitter in improving the secrecy rate in the presence of the eavesdropper, via cooperative signal relaying to the destination or cooperative jamming to the eavesdropper [11]–[13]; (ii) *untrusted relay* from which the source transmitter wishes to keep the information confidential while engaging its help [14], [15]; and (iii) *adversary relay* that helps the eavesdropper, rather than the source transmitter, in decreasing the secrecy rate [16], [17]. On the other hand, proactive eavesdropping in different forms such as pilot contamination attack, false feedback, etc., has also been studied recently [18]–[26]. However, all the aforementioned works focus on the conventional wireless security design based on the information-theoretic secrecy capacity measure, which treats the eavesdroppers as adversaries and thus aims to minimize the information leakage to them. In contrast, for the proactive eavesdropping considered in this paper, the eavesdropper is employed by a legitimate monitor for the different purpose of information surveillance, and how to maximize its eavesdropping rate via optimally designing the spoofing relay strategy is a new problem that has not been studied in the literature.

The rest of this paper is organized as follows. Section II introduces the system model for proactive eavesdropping with

a spoofing relay, and presents the problem formulation for eavesdropping rate maximization. Section III presents the optimal solution for the formulated problem, as well as a low-cost implementation that only requires one power splitter at the legitimate monitor receiver. In Section IV, numerical results are presented to compare the proposed proactive eavesdropping scheme with the two benchmark schemes. Finally, we conclude the paper in Section V.

Notations: In this paper, scalars are denoted by italic letters. Boldface lower- and upper-case letters denote vectors and matrices, respectively. $\mathbb{C}^{M \times N}$ denotes the space of $M \times N$ complex-valued matrices. \mathbf{I} represents an identity matrix, $\mathbf{0}$ and $\mathbf{1}$ denote an all-zero and all-one matrix, respectively. For a matrix \mathbf{A} , its complex conjugate, transpose, Hermitian transpose, and Frobenius norm are respectively denoted as \mathbf{A}^* , \mathbf{A}^T , \mathbf{A}^H , and $\|\mathbf{A}\|_F$. For a vector \mathbf{a} , $\|\mathbf{a}\|$ represents its Euclidean norm. $\text{diag}(\mathbf{a})$ denotes a diagonal matrix with the diagonal elements given in the vector \mathbf{a} . $\mathbf{a} \preceq \mathbf{b}$ means that each element in \mathbf{a} is no greater than that in \mathbf{b} . For a complex number z , $\angle z$ represents its phase, and $\Re(z)$ and $\Im(z)$ denote its real and imaginary parts, respectively. The symbol j represents the imaginary unit of complex numbers, i.e., $j^2 = -1$.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, we consider an information surveillance scenario, where the legitimate monitor \mathbf{E} is intended to overhear a suspicious communication link from source \mathbf{S} to destination \mathbf{D} . We assume that both \mathbf{S} and \mathbf{D} have one single antenna each, whereas \mathbf{E} is equipped with $M \geq 1$ receiving and $N \geq 1$ transmitting antennas. We consider that *adaptive rate transmission* is adopted at \mathbf{S} based on the channel perceived at \mathbf{D} . However, neither \mathbf{S} nor \mathbf{D} is aware of the presence of \mathbf{E} , so that no dedicated coding as in conventional physical-layer security (see e.g., [3] and references therein) is applied to prevent the eavesdropping by \mathbf{E} . On the other hand, the legitimate monitor \mathbf{E} can conduct either passive or proactive eavesdropping, as discussed below.

A. Passive Eavesdropping

With passive eavesdropping, \mathbf{E} remains silent throughout the communication between \mathbf{S} and \mathbf{D} , but tries to decode the information from \mathbf{S} . In this case, the channel capacity of the suspicious link from \mathbf{S} to \mathbf{D} , which is also assumed to be the transmission rate by \mathbf{S} , is given by²

$$R_D = \log_2 \left(1 + \frac{P_S |h_{SD}|^2}{\sigma^2} \right), \quad (1)$$

where h_{SD} is the complex-valued channel gain from \mathbf{S} to \mathbf{D} , P_S is the transmit power by \mathbf{S} , and σ^2 is the power of the additive white Gaussian noise (AWGN) at \mathbf{D} . On the other hand, the capacity of the single-input multiple-output (SIMO)

²The results in this paper can be readily extended to the practical scenario with non-Gaussian signaling [27], by e.g., inserting a gap Γ in the capacity formula (1) as $R_D = \log_2 \left(1 + \frac{P_S |h_{SD}|^2}{\Gamma \sigma^2} \right)$, where $\Gamma > 1$ accounts for the capacity loss due to practical modulation and coding in use.

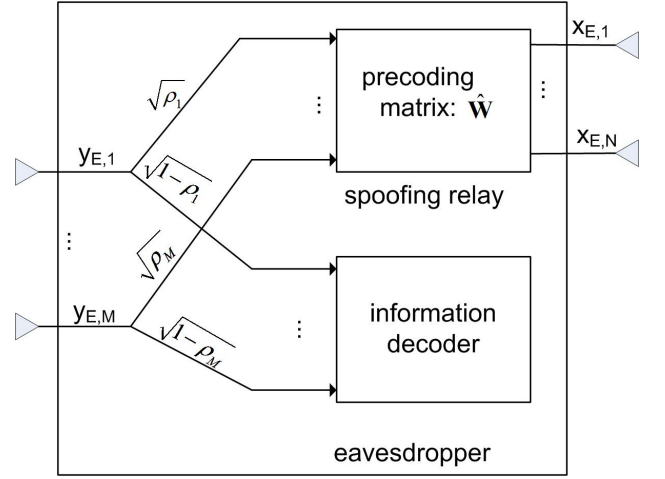


Fig. 2: The architecture of a multi-antenna eavesdropper with spoofing relay.

eavesdropping channel from \mathbf{S} to \mathbf{E} is

$$R_E = \log_2 \left(1 + \frac{P_S \|\mathbf{h}_{SE}\|^2}{\sigma^2} \right), \quad (2)$$

where $\mathbf{h}_{SE} \in \mathbb{C}^{M \times 1}$ denotes the SIMO channel from \mathbf{S} to the M receiving antennas of \mathbf{E} . If $R_E \geq R_D$ or equivalently $\|\mathbf{h}_{SE}\|^2 \geq |h_{SD}|^2$, i.e., the legitimate monitor has a better channel than the suspicious destination, \mathbf{E} can reliably decode the information sent by \mathbf{S} with arbitrarily small error probability. As a result, the effective *eavesdropping rate* is given by $R_{ev} = R_D$. On the other hand, if $R_E < R_D$, or the legitimate monitor has a weaker channel than the suspicious destination, then it is impossible for \mathbf{E} to decode the information from \mathbf{S} without any error. In this case, we define the effective eavesdropping rate as $R_{ev} = 0$.³ Therefore, the effective eavesdropping rate can be expressed as

$$R_{ev} = \begin{cases} R_D, & \text{if } R_E \geq R_D \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

B. Proactive Eavesdropping via Spoofing Relay

In this subsection, we propose a proactive scheme for the legitimate monitor via the spoofing relay technique to enhance the eavesdropping rate over passive eavesdropping. To enable continuous information surveillance with concurrent proactive spoofing relaying, we assume that \mathbf{E} operates in a full-duplex mode with simultaneous information reception and spoofing signal transmission. As will become clear later, one key requirement for the spoofing relay technique is that the excessive time delay of the two effective signal paths (i.e., the direct link from the source to destination and that via the spoofing relay) is much smaller than the symbol duration to avoid causing inter-symbol interference (ISI). Therefore, we assume that the amplify-and-forward (AF) relaying strategy is

³Note that in this case \mathbf{E} may still extract useful information from its received signal. However, in this paper we consider a more stringent requirement that the message from \mathbf{S} needs to be decoded at \mathbf{E} with arbitrarily small error probability to achieve the wireless surveillance goal.

adopted by **E** since it usually has smaller processing delay than other relay processing technique such as decode-and-forward (DF). Therefore, the received signal $\mathbf{y}_E \in \mathbb{C}^{M \times 1}$ by the M receiving antennas of **E** can be expressed as

$$\mathbf{y}_E = \mathbf{h}_{SE} \sqrt{P_S} d_S + \mathbf{H}_{EE} \mathbf{x}_E + \mathbf{n}_E^{(A)}, \quad (4)$$

where $d_S \sim \mathcal{CN}(0, 1)$ denotes the circularly-symmetric complex Gaussian (CSCG) distributed information-bearing symbol sent by **S** with transmit power P_S , $\mathbf{H}_{EE} \in \mathbb{C}^{M \times N}$ represents the loop channel from the N transmitting antennas of **E** to its own M receiving antennas, $\mathbf{x}_E \in \mathbb{C}^{N \times 1}$ denotes the transmitted signal by **E**, and $\mathbf{n}_E^{(A)} \in \mathbb{C}^{M \times 1}$ represents the antenna noise received by **E**. Note that the second term in the expression of \mathbf{y}_E in (4) is due to the full-duplex operation at **E**, which in general couples the input and output signals of **E**. To avoid circuit oscillations in practice as well as to suppress the self-interference from the loop channel, the input and output of **E** must be sufficiently isolated [28]. For ease of exposition, we assume that the ideal input-output isolation is achieved at **E** by designing \mathbf{x}_E that completely nulls the output of the loop-channel, i.e.,

$$\mathbf{H}_{EE} \mathbf{x}_E = \mathbf{0}. \quad (5)$$

Thus, the received signal by **E** in (4) reduces to $\mathbf{y}_E = \mathbf{h}_{SE} \sqrt{P_S} d_S + \mathbf{n}_E^{(A)}$. As shown in Fig. 2, to achieve simultaneous spoofing relaying and information eavesdropping at **E** under the AF operation, the received signal $y_{E,m}$ at each antenna m of **E** is split into two parts, one for constructive/destructive information relaying aiming to enhance/degrade the effective channel of the suspicious link from **S** to **D**, and the other for information decoding so as to eavesdrop the message sent by **S**. Denote by $0 \leq \rho_m \leq 1$ the power splitting ratio of antenna m , the signal vector split for information relaying can be expressed as

$$\mathbf{y}'_E = \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{y}_E = \text{diag}(\sqrt{\boldsymbol{\rho}}) \left(\mathbf{h}_{SE} \sqrt{P_S} d_S + \mathbf{n}_E^{(A)} \right), \quad (6)$$

where $\boldsymbol{\rho} = [\rho_1, \dots, \rho_M]^T$ represents the power splitting vector, and $\sqrt{\boldsymbol{\rho}}$ represents a vector obtained by taking element-wise square root. The transmitted signal $\mathbf{x}_E \in \mathbb{C}^{N \times 1}$ by the N transmitting antennas of **E** can then be expressed as

$$\mathbf{x}_E = \hat{\mathbf{W}} \left(\mathbf{y}'_E + \mathbf{n}_E^{(R)} \right) \quad (7)$$

$$\approx \hat{\mathbf{W}} \left(\text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE} \sqrt{P_S} d_S + \mathbf{n}_E^{(R)} \right), \quad (8)$$

where $\hat{\mathbf{W}} \in \mathbb{C}^{N \times M}$ is the relay precoding matrix at **E**, and $\mathbf{n}_E^{(R)} \sim \mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_M)$ denotes the processing noise introduced during the relaying operation at **E**, which is assumed to dominate over the antenna noise $\mathbf{n}_E^{(A)}$; thus, $\mathbf{n}_E^{(A)}$ is ignored in (8). The transmit power by **E** is thus given by

$$\mathbb{E} [\|\mathbf{x}_E\|^2] = P_S \|\hat{\mathbf{W}} \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE}\|^2 + \sigma^2 \|\hat{\mathbf{W}}\|_F^2. \quad (9)$$

By assuming that the processing delay due to the AF relaying at **E** is much smaller than the symbol duration, and hence is

negligible, the signal received at **D** can be expressed as

$$y_D = h_{SD} \sqrt{P_S} d_S + \mathbf{h}_{ED}^H \mathbf{x}_E + n_D \quad (10)$$

$$= \underbrace{(h_{SD} + \mathbf{h}_{ED}^H \hat{\mathbf{W}} \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE})}_{\tilde{h}_{SD}} \sqrt{P_S} d_S + \underbrace{\mathbf{h}_{ED}^H \hat{\mathbf{W}} \mathbf{n}_E^{(R)}}_{\tilde{n}_D} + n_D, \quad (11)$$

where $\mathbf{h}_{ED}^H \in \mathbb{C}^{1 \times N}$ denotes the multiple-input single-output (MISO) channel from the N transmitting antennas of **E** to **D**, and $n_D \sim \mathcal{CN}(0, \sigma^2)$ is the AWGN at **D**. It is observed from (11) that by adjusting the power splitting ratio vector $\boldsymbol{\rho}$ and the precoding matrix $\hat{\mathbf{W}}$, the legitimate monitor **E** is able to alter the effective channel \tilde{h}_{SD} of the suspicious link from **S** to **D**. The capacity of the suspicious link is thus given by $\tilde{R}_D = \log_2(1 + \tilde{\gamma}_D)$, where $\tilde{\gamma}_D$ is the effective SNR at **D**, which can be obtained from (11) as a function of $\boldsymbol{\rho}$ and $\hat{\mathbf{W}}$ as

$$\tilde{\gamma}_D(\boldsymbol{\rho}, \hat{\mathbf{W}}) = \frac{\left| h_{SD} + \mathbf{h}_{ED}^H \hat{\mathbf{W}} \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE} \right|^2 \tilde{P}_S}{1 + \|\mathbf{h}_{ED}^H \hat{\mathbf{W}}\|^2}, \quad (12)$$

where $\tilde{P}_S \triangleq P_S / \sigma^2$ represents the transmit SNR by **S**. Note that the term $\|\mathbf{h}_{ED}^H \hat{\mathbf{W}}\|^2$ in the denominator of (12) is due to the noise amplification by **E**.

On the other hand, at the information decoder of **E**, the split signal based on which the message from **S** is decoded can be expressed as

$$\tilde{\mathbf{y}}_E = \text{diag}(\sqrt{\mathbf{1} - \boldsymbol{\rho}}) \mathbf{h}_{SE} \sqrt{P_S} d_S + \mathbf{n}_E^{(D)}, \quad (13)$$

where $\mathbf{n}_E^{(D)} \sim \mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_M)$ denotes the AWGN at the information decoder of **E**. Thus, the information rate achievable by **E** with the optimal maximal ratio combining (MRC) over all the M signal branches is $\tilde{R}_E = \log_2(1 + \tilde{\gamma}_E)$, where $\tilde{\gamma}_E$ is the SNR as a function of $\boldsymbol{\rho}$ given by

$$\tilde{\gamma}_E(\boldsymbol{\rho}) = \frac{\mathbf{h}_{SE}^H \text{diag}(\mathbf{1} - \boldsymbol{\rho}) \mathbf{h}_{SE} \tilde{P}_S}{(\|\mathbf{h}_{SE}\|^2 - \mathbf{h}_{SE}^H \text{diag}(\boldsymbol{\rho}) \mathbf{h}_{SE}) \tilde{P}_S}. \quad (14)$$

To study the fundamental performance limit achievable by the legitimate monitor, we assume that perfect channel state information (CSI) of all links is available at **E**. Note that in practice, the loop channel \mathbf{H}_{EE} can be estimated beforehand at the legitimate monitor. On the other hand, the channels \mathbf{h}_{SE} and \mathbf{h}_{ED} could be estimated at the legitimate monitor by overhearing the pilot signals sent by **S** and **D**, respectively. For the suspicious link channel h_{SD} , it could be obtained by overhearing the channel feedback sent from **D** to **S**.

C. Problem Formulation

The objective of the legitimate monitor **E** is to jointly optimize the power splitting ratio vector $\boldsymbol{\rho}$ and the relay precoding matrix $\hat{\mathbf{W}}$ so that the eavesdropping rate is maximized. Based

on the definition in (3), the problem can be formulated as

$$(P1) : \begin{cases} \max_{\tilde{\mathbf{W}}, \boldsymbol{\rho}} & \tilde{R}_D(\boldsymbol{\rho}, \tilde{\mathbf{W}}) \\ \text{s.t.} & \tilde{R}_E(\boldsymbol{\rho}) \geq \tilde{R}_D(\boldsymbol{\rho}, \tilde{\mathbf{W}}) \\ & \mathbf{H}_{EE} \tilde{\mathbf{W}} = \mathbf{0}, \\ & \mathbf{0} \preceq \boldsymbol{\rho} \preceq \mathbf{1}, \\ & \tilde{P}_S \|\tilde{\mathbf{W}} \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE}\|^2 + \|\tilde{\mathbf{W}}\|_F^2 \leq \tilde{P}_E, \end{cases} \quad (15)$$

where the zero-forcing (ZF) constraint $\mathbf{H}_{EE} \tilde{\mathbf{W}} = \mathbf{0}$ follows from (5) and (7), and \tilde{P}_E represents the maximum power available at **E** normalized by the noise power σ^2 . (P1) is a non-convex optimization problem. However, by exploiting its structure, the optimal solution can be efficiently obtained, as shown next.

III. OPTIMAL SOLUTION

To obtain the optimal solution to (P1), we first consider the ZF constraint $\mathbf{H}_{EE} \tilde{\mathbf{W}} = \mathbf{0}$. This implies that the precoding matrix $\tilde{\mathbf{W}}$ must lie in the null space of \mathbf{H}_{EE} . Let the (reduced) singular value decomposition (SVD) of \mathbf{H}_{EE} be expressed as $\mathbf{H}_{EE} = \mathbf{U}_1 \mathbf{\Lambda}_1 \mathbf{V}_1^H$, where $\mathbf{U}_1 \in \mathbb{C}^{M \times r_1}$ and $\mathbf{V}_1 \in \mathbb{C}^{N \times r_1}$ contain the r_1 orthonormal left and right singular vectors of \mathbf{H}_{EE} , respectively, with $r_1 \leq \min\{M, N\}$ denoting the matrix rank of \mathbf{H}_{EE} , and $\mathbf{\Lambda}_1 = \text{diag}(\lambda_1, \dots, \lambda_{r_1})$ contains the r_1 positive singular values of \mathbf{H}_{EE} . Further denote by $\mathbf{V}_0 \in \mathbb{C}^{N \times r_0}$ with $r_0 \triangleq N - r_1$ the orthogonal complement of \mathbf{V}_1 , i.e., the concatenated matrix $\mathbf{V} \triangleq [\mathbf{V}_1 \ \mathbf{V}_0]$ forms an orthonormal basis for the N -dimensional space with $\mathbf{V}^H \mathbf{V} = \mathbf{I}_N$. The precoding matrix $\tilde{\mathbf{W}}$ satisfying the ZF constraint in (P1) can then be expressed as

$$\tilde{\mathbf{W}} = \mathbf{V}_0 \mathbf{W}, \quad (16)$$

where $\mathbf{W} \in \mathbb{C}^{r_0 \times M}$ denotes the new matrix to be designed. It is not difficult to observe that in order for the ZF constraint to be feasible, we must have $r_0 \geq 1$, or equivalently the rank of \mathbf{H}_{EE} must satisfy $r_1 < N$. Since $r_1 \leq \min\{M, N\}$, one sufficient (but not necessary) condition is thus $N > M$, i.e., more antennas at **E** should be allocated for transmission than that for reception.

By substituting (16) into (12), the effective SNR at **D** as a function of $\boldsymbol{\rho}$ and \mathbf{W} can be expressed as

$$\tilde{\gamma}_D(\boldsymbol{\rho}, \mathbf{W}) = \frac{|h_{SD} + \hat{\mathbf{h}}_{ED}^H \mathbf{W} \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE}|^2 \tilde{P}_S}{1 + \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}\|^2}, \quad (17)$$

where $\hat{\mathbf{h}}_{ED} \triangleq \mathbf{V}_0^H \mathbf{h}_{ED}$ denotes the projected channel of \mathbf{h}_{ED} onto the null space of \mathbf{H}_{EE} . Furthermore, since the link capacity \tilde{R}_D and \tilde{R}_E monotonically increase with the SNR $\tilde{\gamma}_D(\boldsymbol{\rho}, \mathbf{W})$ and $\tilde{\gamma}_E(\boldsymbol{\rho})$, respectively, (P1) thus reduces to

$$(P2) : \begin{cases} \max_{\mathbf{W}, \boldsymbol{\rho}} & \tilde{\gamma}_D(\boldsymbol{\rho}, \mathbf{W}) \\ \text{s.t.} & \tilde{\gamma}_E(\boldsymbol{\rho}) \geq \tilde{\gamma}_D(\boldsymbol{\rho}, \mathbf{W}) \\ & \mathbf{0} \preceq \boldsymbol{\rho} \preceq \mathbf{1}, \\ & \tilde{P}_S \|\mathbf{W} \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE}\|^2 + \|\mathbf{W}\|_F^2 \leq \tilde{P}_E, \end{cases} \quad (18)$$

where the last constraint follows from the equality $\|\hat{\mathbf{W}} \mathbf{a}\|^2 = \|\mathbf{W} \mathbf{a}\|^2$, $\forall \mathbf{a} \in \mathbb{C}^{M \times 1}$, and $\|\hat{\mathbf{W}}\|_F^2 = \|\mathbf{W}\|_F^2$ due to the fact that $\mathbf{V}_0^H \mathbf{V}_0 = \mathbf{I}$. Note that (P2) is equivalent to (P1) in the sense that they have the same optimal value (except the logarithmic transformation between rate and SNR), and their optimal solutions are related by the simple linear transformation equation (16). (P2) is still a non-convex optimization problem, due to the non-concave objective function as well as the non-convexity of the first constraint. However, by exploiting the special structure of the SNR expressions for $\tilde{\gamma}_E(\boldsymbol{\rho})$ and $\tilde{\gamma}_D(\boldsymbol{\rho}, \mathbf{W})$, the optimal solution to (P2) can be efficiently obtained. Specifically, by firstly optimizing the precoding matrix \mathbf{W} with fixed power splitting vector $\boldsymbol{\rho}$, the maximum and minimum achievable SNRs (or equivalently the achievable SNR range) at **D** with fixed $\boldsymbol{\rho}$ can be obtained. The problem (P2) then reduces to finding the optimal power splitting vector $\boldsymbol{\rho}$, as formulated in (P3) in Section III-C. The details are given next.

A. Maximum Achievable SNR at **D** with Fixed $\boldsymbol{\rho}$

To obtain the optimal solution to (P2), it is noted that the SNR $\tilde{\gamma}_E(\boldsymbol{\rho})$ at **E** only depends on the power splitting ratio vector $\boldsymbol{\rho}$, rather than the precoding matrix \mathbf{W} . Thus, for any fixed $\boldsymbol{\rho}$, we first obtain the maximum achievable SNR at **D**, denoted as $\tilde{\gamma}_D^{\max}(\boldsymbol{\rho})$, by optimizing \mathbf{W} as

$$\tilde{\gamma}_D^{\max}(\boldsymbol{\rho}) \triangleq \begin{cases} \max_{\mathbf{W}} & \tilde{\gamma}_D(\boldsymbol{\rho}, \mathbf{W}) \\ \text{s.t.} & \tilde{P}_S \|\mathbf{W} \hat{\mathbf{h}}_{SE}\|^2 + \|\mathbf{W}\|_F^2 \leq \tilde{P}_E, \end{cases} \quad (19)$$

where we have defined $\hat{\mathbf{h}}_{SE} \triangleq \text{diag}(\sqrt{\boldsymbol{\rho}}) \mathbf{h}_{SE}$.

Theorem 1. The optimal solution to problem (19) is

$$\mathbf{W}_1^* = \sqrt{\mu_1^*} e^{j\angle h_{SD}} \tilde{\mathbf{h}}_{ED} \tilde{\mathbf{h}}_{SE}^H, \quad (20)$$

where $\tilde{\mathbf{h}}_{ED} \triangleq \hat{\mathbf{h}}_{ED} / \|\hat{\mathbf{h}}_{ED}\|$, $\tilde{\mathbf{h}}_{SE} \triangleq \hat{\mathbf{h}}_{SE} / \|\hat{\mathbf{h}}_{SE}\|$, and $\mu_1^* = \min \left\{ \frac{\|\hat{\mathbf{h}}_{SE}\|^2}{|h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2}, \frac{\tilde{P}_E}{\tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2 + 1} \right\}$. Furthermore, the corresponding optimal value is given by (21) shown at the top of the next page.

Proof: Please refer to Appendix A. ■

Theorem 1 shows that in order to maximize the SNR at **D**, the precoding matrix \mathbf{W} at **E** should be chosen such that the two signal paths from **S** to **D**, namely the direct link and that via the monitor relaying, add constructively, i.e., $\angle h_{SD} = \angle \hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}$. We term such a strategy of the spoofing relay as *constructive information forwarding*, since it helps enhance the effective channel of the suspicious link from **S** to **D**. Furthermore, (20) shows that the optimal relay precoding matrix \mathbf{W}_1^* is given by a rank-1 matrix, with a simple MRC-based linear combining (by the term $\tilde{\mathbf{h}}_{SE}^H$) of the output of the power splitters cascaded by a maximal-ratio transmission (MRT) beamforming (by the term $\tilde{\mathbf{h}}_{ED}$) [27].

It is also noted from (21) that for any fixed power splitting ratios $\boldsymbol{\rho}$, the maximum achievable SNR $\tilde{\gamma}_D^{\max}(\boldsymbol{\rho})$ at **D** depends on $\boldsymbol{\rho}$ only via the term $\|\hat{\mathbf{h}}_{SE}\|^2 = \mathbf{h}_{SE}^H \text{diag}(\boldsymbol{\rho}) \mathbf{h}_{SE}$. In particular, if $\boldsymbol{\rho} = \mathbf{0}$, i.e., no information forwarding is applied at **E**, we have $\tilde{\gamma}_D^{\max}(\mathbf{0}) = \tilde{P}_S |h_{SD}|^2$, which corresponds to the special case of passive eavesdropping previously discussed

$$\tilde{\gamma}_D^{\max}(\rho) = \begin{cases} \left(1 + \frac{\|\hat{\mathbf{h}}_{SE}\|^2}{|h_{SD}|^2}\right) \tilde{P}_S |h_{SD}|^2, & \text{if } \frac{\|\hat{\mathbf{h}}_{SE}\|^2}{|h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2} \leq \frac{\tilde{P}_E}{\tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2 + 1} \\ \frac{\left(\sqrt{\tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2 + 1} + \sqrt{\tilde{P}_E \|\hat{\mathbf{h}}_{SE}\|^2 \|\hat{\mathbf{h}}_{ED}\|^2 / |h_{SD}|^2}\right)^2 \tilde{P}_S |h_{SD}|^2}{\tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 + 1}, & \text{otherwise.} \end{cases} \quad (21)$$

in Section II-A. On the other hand, if $\rho = 1$ and P_E is sufficiently large, we have $\tilde{\gamma}_D^{\max}(1) = \tilde{P}_S(|h_{SD}|^2 + \|\hat{\mathbf{h}}_{SE}\|^2)$. This results in the maximum SNR achievable at **D** which is equivalent to that achieved by MRC-based signal detection jointly performed at **E** and **D**. However, in this case, there is no signal split for information decoding at the legitimate monitor and thus the effective eavesdropping rate will be zero.

B. Minimum Achievable SNR at **D** with Fixed ρ

Next, for fixed power splitting ratios ρ , we study the minimum achievable SNR at **D**, denoted as $\tilde{\gamma}_D^{\min}(\rho)$, which can be obtained by solving the following optimization problem,

$$\tilde{\gamma}_D^{\min}(\rho) \triangleq \begin{cases} \min_{\mathbf{W}} & \tilde{\gamma}_D(\rho, \mathbf{W}) \\ \text{s.t.} & \tilde{P}_S \|\mathbf{W} \hat{\mathbf{h}}_{SE}\|^2 + \|\mathbf{W}\|_F^2 \leq \tilde{P}_E. \end{cases} \quad (22)$$

Theorem 2. *The optimal solution to problem (22) is*

$$\mathbf{W}_2^* = -e^{j\angle h_{SD}} \tilde{\mathbf{h}}_{ED} \left(\sqrt{z_1^*} \tilde{\mathbf{h}}_{SE} + \sqrt{z_2^*} \tilde{\mathbf{h}}_{SE}^\perp \right)^H, \quad (23)$$

where $\tilde{\mathbf{h}}_{SE}^\perp$ is any unit-norm vector that is orthogonal to $\tilde{\mathbf{h}}_{SE}$, i.e., $\tilde{\mathbf{h}}_{SE}^H \tilde{\mathbf{h}}_{SE}^\perp = 0$, and z_1^* and z_2^* are the optimal solution to the following problem,

$$\tilde{\gamma}_D^{\min}(\rho) \triangleq \begin{cases} \min_{z_1, z_2} & \tilde{\gamma}_D''(z_1, z_2) \triangleq \frac{(|h_{SD}| - \sqrt{z_1} \|\tilde{\mathbf{h}}_{ED}\| \|\tilde{\mathbf{h}}_{SE}\|)^2 \tilde{P}_S}{1 + \|\tilde{\mathbf{h}}_{ED}\|^2 (z_1 + z_2)} \\ \text{s.t.} & (1 + \tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2) z_1 + z_2 \leq \tilde{P}_E, \\ & z_1, z_2 \geq 0. \end{cases} \quad (24)$$

Proof: Please refer to Appendix B. ■

Theorem 2 shows that in order to minimize the SNR at **D**, the precoding matrix \mathbf{W} by **E** should be chosen such that the two effective signal paths from **S** to **D** add destructively, i.e., $\angle h_{SD} = \pi + \angle \hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}$. Such a strategy at **E** is termed as *destructive information forwarding*, which degrades the effective channel of the suspicious link from **S** to **D**. Furthermore, similar to \mathbf{W}_1^* for maximizing SNR at **D**, \mathbf{W}_2^* in (23) for SNR minimization at **D** is also a rank-one matrix with a similar structure. However, although the MRT-based transmit beamforming still applies, the preceding combining vector for the power-splitting output is in general given by a linear combination of the MRC combining $\hat{\mathbf{h}}_{SE}$ and its orthogonal vector $\hat{\mathbf{h}}_{SE}^\perp$. Note that although the power allocated along the direction $\hat{\mathbf{h}}_{SE}^\perp$ does not forward any destructive source signal to **D**, it also contributes to the SNR degradation at **D** via *jamming*, i.e., amplifying the noise at **E** to **D**. Thus, the optimal relaying strategy by **E** for SNR minimization at **D** in general involves both destructive information forwarding and jamming.

Theorem 3. *The optimal solution and the corresponding optimal value of problem (24) are respectively given by (25) and (26) shown at the top of the next page, where*

$$\begin{aligned} Z_1 &\triangleq \frac{(1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)^2}{\tilde{P}_S^2 |h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2 \|\hat{\mathbf{h}}_{SE}\|^2}, \\ Z_2 &\triangleq \tilde{P}_E - (1 + \tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2) Z_1, \\ C_1 &\triangleq \tilde{P}_S \left(\tilde{P}_S \tilde{P}_E |h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2 - (1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)^2 \right). \end{aligned} \quad (27)$$

$$(28)$$

Proof: Please refer to Appendix C. ■

The results in (25) and (26) show that if both \tilde{P}_E and the split power $\|\hat{\mathbf{h}}_{SE}\|^2$ for information relaying are sufficiently large (corresponding to the first case in (25) and (26)), the destructive relaying signal from **E** is able to completely cancel the signal of the direct path from **S** at **D**, and thus makes the SNR at **D** equal to zero. In this case, no dedicated jamming is needed ($z_2^* = 0$) for SNR minimization at **D**. On the other hand, if destructive information relaying is unable to drive the SNR at **D** to zero with the given transmit power of **E**, both destructive relaying and jamming are in general needed for the SNR degradation at **D**. Furthermore, similar to that in (21), the minimum achievable SNR $\tilde{\gamma}_D^{\min}(\rho)$ in (26) depends on ρ only via the term $\|\hat{\mathbf{h}}_{SE}\|^2$. In particular, if $\rho = 0$, i.e., no information forwarding is applied at **E**, we have $\tilde{\gamma}_D^{\min}(0) = \tilde{P}_S |h_{SD}|^2 / (1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)$, which corresponds to jamming (merely noise amplification) with full power of **E**.

C. Optimal Solution to (P2)

Now we obtain the optimal solution to problem (P2) based on the above results. Since $\tilde{\gamma}_D(\rho, \mathbf{W})$ given in (17) is a continuous function of \mathbf{W} , for any fixed power splitting ratio vector $0 \leq \rho \leq 1$, the set of achievable SNRs at **D** is given by the interval $[\tilde{\gamma}_D^{\min}(\rho), \tilde{\gamma}_D^{\max}(\rho)]$, with $\tilde{\gamma}_D^{\max}(\rho)$ and $\tilde{\gamma}_D^{\min}(\rho)$ denoting the maximum and minimum achievable SNRs given in closed-forms by (21) and (26), respectively. As a result, (P2) reduces to finding the optimal power splitting ratios ρ via solving the following optimization problem,

$$(P3) : \begin{cases} \max_{\rho, \tilde{\gamma}_D} & \tilde{\gamma}_D \\ \text{s.t.} & \tilde{\gamma}_D^{\min}(\rho) \leq \tilde{\gamma}_D \leq \tilde{\gamma}_D^{\max}(\rho) \\ & \tilde{\gamma}_D \leq \tilde{\gamma}_E(\rho) \\ & 0 \leq \rho \leq 1. \end{cases} \quad (29)$$

Theorem 4. *Without loss of optimality to (P3), the power splitting ratio vector ρ can be expressed as $\rho = \rho 1$ for $0 \leq \rho \leq 1$.*

Proof: Please refer to Appendix D. ■

Theorem 4 shows that *uniform power splitting* (UPS), i.e., all the M receiving antennas at **E** employ the same

$$(z_1^*, z_2^*) = \begin{cases} \left(\frac{|h_{SD}|^2}{\|\hat{\mathbf{h}}_{ED}\|^2 \|\hat{\mathbf{h}}_{SE}\|^2}, 0 \right), & \text{if } \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 > \tilde{P}_S |h_{SD}|^2 \text{ and } \|\hat{\mathbf{h}}_{SE}\|^2 \geq \frac{|h_{SD}|^2}{\tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 - \tilde{P}_S |h_{SD}|^2}, \\ (Z_1, Z_2), & \text{if } \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 \leq \tilde{P}_S |h_{SD}|^2 \text{ and } \|\hat{\mathbf{h}}_{SE}\|^2 C_1 > (1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)^2 \\ \left(\frac{\tilde{P}_E}{1 + \tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2}, 0 \right), & \text{otherwise,} \end{cases} \quad (25)$$

$$\tilde{\gamma}_D^{\min}(\rho) = \begin{cases} 0, & \text{if } \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 > \tilde{P}_S |h_{SD}|^2 \text{ and } \|\hat{\mathbf{h}}_{SE}\|^2 \geq \frac{|h_{SD}|^2}{\tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 - \tilde{P}_S |h_{SD}|^2}, \\ \frac{\tilde{P}_S |h_{SD}|^2}{1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2} - 1, & \text{if } \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 \leq \tilde{P}_S |h_{SD}|^2 \text{ and } \|\hat{\mathbf{h}}_{SE}\|^2 C_1 > (1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)^2 \\ \frac{(\sqrt{1 + \tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2} - \frac{\|\hat{\mathbf{h}}_{ED}\| \|\hat{\mathbf{h}}_{SE}\| \sqrt{\rho \tilde{P}_E}}{|h_{SD}|})^2 \tilde{P}_S |h_{SD}|^2}{1 + \tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2}, & \text{otherwise.} \end{cases} \quad (26)$$

power splitting ratio, is optimal to (P3). By substituting with $\rho = \rho_1$ and after some simple manipulations, $\tilde{\gamma}_E(\rho)$ in (14) and $\tilde{\gamma}_D^{\max}(\rho)$ in (21) respectively reduce to the uni-variate functions

$$\tilde{\gamma}_E(\rho) = (1 - \rho) \|\mathbf{h}_{SE}\|^2 \tilde{P}_S, \quad (30)$$

$$\tilde{\gamma}_D^{\max}(\rho) = \begin{cases} \left(1 + \frac{\rho \|\mathbf{h}_{SE}\|^2}{|h_{SD}|^2} \right) \tilde{P}_S |h_{SD}|^2, & 0 \leq \rho \leq \rho_1 \\ \frac{(\sqrt{1 + \rho \|\mathbf{h}_{SE}\|^2} \tilde{P}_S + \frac{\|\mathbf{h}_{SE}\| \|\hat{\mathbf{h}}_{ED}\| \sqrt{\rho \tilde{P}_E}}{|h_{SD}|})^2 \tilde{P}_S |h_{SD}|^2}{1 + \rho \|\mathbf{h}_{SE}\|^2 \tilde{P}_S + \|\hat{\mathbf{h}}_{ED}\|^2 \tilde{P}_E}, & \rho_1 < \rho \leq 1, \end{cases} \quad (31)$$

where $\rho_1 \triangleq \min \left\{ 1, \frac{-1 + \sqrt{1 + 4 \tilde{P}_S \tilde{P}_E |h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2}}{2 \|\mathbf{h}_{SE}\|^2 \tilde{P}_S} \right\}$. Furthermore, $\tilde{\gamma}_D^{\min}(\rho)$ in (26) reduces to the uni-variate function (32) shown at the top of the next page, where $\rho_2 \triangleq \min \left\{ 1, \frac{|h_{SD}|^2}{\|\mathbf{h}_{SE}\|^2 (\tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 - \tilde{P}_S |h_{SD}|^2)} \right\}$, and $\rho_3 = C_2$ if $0 \leq C_2 \leq 1$, and $\rho_3 = 1$ otherwise, with $C_2 \triangleq \frac{\|\mathbf{h}_{SE}\|^2 \tilde{P}_S (\tilde{P}_S \tilde{P}_E |h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2 - (1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)^2)}{\|\mathbf{h}_{SE}\|^2 \tilde{P}_S (\tilde{P}_S \tilde{P}_E |h_{SD}|^2 \|\hat{\mathbf{h}}_{ED}\|^2 - (1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2)^2)}$.

As a result, (P3) reduces to finding the optimal single power splitting ratio ρ via solving

$$(P3') : \begin{cases} \max_{0 \leq \rho \leq 1, \tilde{\gamma}_D} & \tilde{\gamma}_D \\ \text{s.t.} & \tilde{\gamma}_D^{\min}(\rho) \leq \tilde{\gamma}_D \leq \tilde{\gamma}_D^{\max}(\rho) \\ & \tilde{\gamma}_D \leq \tilde{\gamma}_E(\rho). \end{cases} \quad (33)$$

By noticing that $\tilde{\gamma}_E(\rho)$ in (30) is a linear decreasing function of ρ , (P3') is essentially equivalent to finding the “best” intersection point between the line $\tilde{\gamma}_E(\rho)$ and the set

$$\mathcal{X} \triangleq \{(\gamma, \rho) | 0 \leq \rho \leq 1, \tilde{\gamma}_D^{\min}(\rho) \leq \gamma \leq \tilde{\gamma}_D^{\max}(\rho)\} \quad (34)$$

in the γ - ρ plane, which can be optimally solved by separately considering the following three cases, as illustrated in Fig. 3.

Case 1: $\tilde{\gamma}_D^{\max}(0) < \tilde{\gamma}_E(0)$ or $|h_{SD}|^2 < \|\mathbf{h}_{SE}\|^2$ as illustrated in Fig. 3(a). In this case, the legitimate monitor **E** has a better channel than the suspicious receiver **D**. Intuitively, **E** should perform constructive information forwarding to enhance the effective channel of **D** so as to increase the eavesdropping rate. It follows from Fig. 3(a) that the optimal solution to (P2) is given by the intersection point of the two curves $\tilde{\gamma}_D^{\max}(\rho)$ and $\tilde{\gamma}_E(\rho)$. As $\tilde{\gamma}_D^{\max}(\rho)$ and $\tilde{\gamma}_E(\rho)$ are monotonically increasing and decreasing functions over $0 \leq \rho \leq 1$, respectively, and $\tilde{\gamma}_D^{\max}(1) > \tilde{\gamma}_E(1) = 0$, the

equation $\tilde{\gamma}_D^{\max}(\rho) = \tilde{\gamma}_E(\rho)$ has one unique solution ρ^* , which can be efficiently obtained via bisection method.

Furthermore, if **E** has sufficiently large power \tilde{P}_E , ρ^* can be obtained in closed-form, as given in the following lemma.

Lemma 1. *If $\alpha \triangleq \frac{\|\mathbf{h}_{SE}\|^2}{|h_{SD}|^2} > 1$ and $\tilde{P}_E \geq \frac{\alpha(1 + \|\mathbf{h}_{SE}\|^2 \tilde{P}_S)}{\|\hat{\mathbf{h}}_{ED}\|^2}$, the optimal solution to (P3') is $\rho^* = \frac{1}{2} \left(1 - \frac{1}{\alpha} \right)$, and the SNRs of both **D** and **E** are $\tilde{\gamma}_D^* = \tilde{\gamma}_E^* = \frac{\|\mathbf{h}_{SE}\|^2 + |h_{SD}|^2}{2} \tilde{P}_S$.*

Proof: Lemma 1 directly follows by noticing that with sufficiently large \tilde{P}_E as specified in the lemma, $\tilde{\gamma}_D^{\max}(\rho)$ in (31) reduces to the linear function of ρ since $\rho_1 = 1$. ■

Lemma 1 shows that by employing constructive relaying with the optimal power splitting ratio ρ^* , **E** is able to increase the eavesdropping rate as compared to passive eavesdropping since $\tilde{\gamma}_D^* > |h_{SD}|^2 \tilde{P}_S$. Furthermore, as α increases, more power should be split at **E** for constructive relaying to enhance the suspicious link SNR. In the extreme case when $\alpha \rightarrow \infty$, i.e., the eavesdropper's link is much stronger than the suspicious user's link, half of the power of the received signal at **E** should be split for information relaying, and the other half for information decoding (eavesdropping).

Case 2: $\tilde{\gamma}_D^{\min}(0) \leq \tilde{\gamma}_E(0) \leq \tilde{\gamma}_D^{\max}(0)$ or $\frac{|h_{SD}|^2}{1 + \|\hat{\mathbf{h}}_{ED}\|^2 \tilde{P}_E} \leq \|\mathbf{h}_{SE}\|^2 \leq |h_{SD}|^2$, as illustrated in Fig. 3(b). In this case, the eavesdropping link is worse than the suspicious link, but it becomes better if jamming with full power is applied at **E** to degrade the suspicious link. It follows from Fig. 3(b) that the optimal solution to (P3') is $\rho^* = 0$, i.e., no information forwarding and only jamming should be applied at **E**, where the normalized jamming power is given by $\tilde{P}_E^* = \frac{1}{\|\hat{\mathbf{h}}_{ED}\|^2} \left(\frac{|h_{SD}|^2}{\|\mathbf{h}_{SE}\|^2} - 1 \right)$ so as to degrade the suspicious link SNR to the same level as that at **E**. In this case, the SNR at both **D** and **E** is $\gamma_D^* = \gamma_E^* = \|\mathbf{h}_{SE}\|^2 \tilde{P}_S$.

Case 3: $\tilde{\gamma}_E(0) < \tilde{\gamma}_D^{\min}(0)$ or $\|\mathbf{h}_{SE}\|^2 < \frac{|h_{SD}|^2}{1 + \|\hat{\mathbf{h}}_{ED}\|^2 \tilde{P}_E}$, as illustrated in Fig. 3(c). In this case, the legitimate monitor's link is worse than the suspicious user's link even after jamming with full power by **E**. Therefore, destructive information forwarding and jamming should be both applied at **E** to further degrade the suspicious link SNR. It follows from Fig. 3(c) that the optimal solution ρ^* to (P3') is obtained by solving $\tilde{\gamma}_D^{\min}(\rho) = \tilde{\gamma}_E(\rho)$ in the interval $0 \leq \rho \leq 1$, which can be reduced to a quartic equation and hence solved efficiently. Note that if more than one solutions exist, the one with the smallest magnitude is the optimal solution. On the other hand,

$$\tilde{\gamma}_D^{\min}(\rho) = \begin{cases} 0, & \rho_2 < \rho \leq 1 \text{ for } \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 > \tilde{P}_S |h_{SD}|^2 \\ \frac{\tilde{P}_S |h_{SD}|^2}{1 + \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2} - 1, & \rho_3 < \rho \leq 1 \text{ for } \tilde{P}_E \|\hat{\mathbf{h}}_{ED}\|^2 \leq \tilde{P}_S |h_{SD}|^2 \\ \frac{(\sqrt{1 + \rho \|\mathbf{h}_{SE}\|^2 \tilde{P}_S} - \frac{\|\mathbf{h}_{SE}\| \|\hat{\mathbf{h}}_{ED}\|}{|h_{SD}|} \sqrt{\rho \tilde{P}_E})^2 \tilde{P}_S |h_{SD}|^2}{1 + \rho \|\mathbf{h}_{SE}\|^2 \tilde{P}_S + \|\hat{\mathbf{h}}_{ED}\|^2 \tilde{P}_E}, & \text{otherwise,} \end{cases} \quad (32)$$

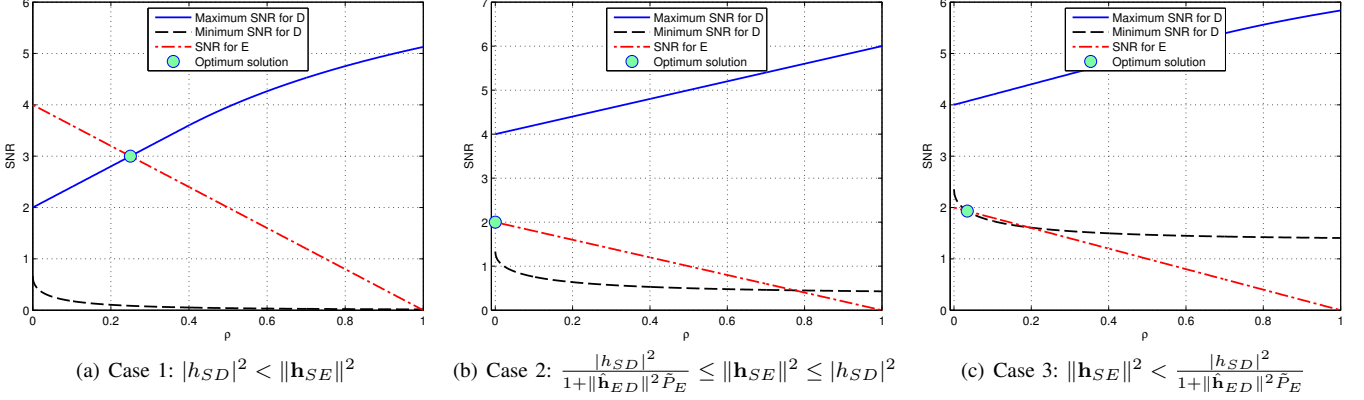


Fig. 3: Three cases for the optimal power splitting solution.

if no solution exists, it implies that problem (P3'), and hence (P1), is infeasible, i.e., the legitimate monitor is unable to degrade the suspicious user transmission rate to be decodable by **E** with its given transmit power.

D. Low-Cost Implementation with One Single Power Splitter

The solution obtained in the preceding subsection in general leads to positive power splitting ratios at all receiving antennas of **E** (except for Case 2 where jamming only is optimal), i.e., $\rho_m > 0, \forall m$; thus, in total M power splitters need to be equipped at **E**, which could be costly in practice. In this subsection, we show that for practical implementation, one single power splitter is sufficient to achieve optimal eavesdropping, regardless of the number of receiving antennas M .

Theorem 5. *There exists an optimal solution to (P3) such that the power splitting ratios $\{\rho_m\}_{m=1}^M$ are given by*

$$\rho_m = \begin{cases} \rho, & m = m^* \\ 0 \text{ or } 1, & m \neq m^*. \end{cases} \quad (35)$$

Proof: Please refer to Appendix E. ■

Note that Appendix E gives a constructive proof of Theorem 5, where the optimal power splitting ratio vector satisfying (35) is obtained in closed-form (56) based on the optimal uniform power splitting vector to problem (P3). Therefore, in terms of computational complexity, the (semi-)binary power splitting solution in Theorem 5 is comparable to that of the uniform power splitting solution obtained in the preceding subsection, which are both quite efficient since they only require solving either a bisection search problem (for Case 1) or a quartic equation (for Case 3). However, in terms of practical implementation, the solution given in Theorem 5 is more cost-effective since it requires only one power splitter

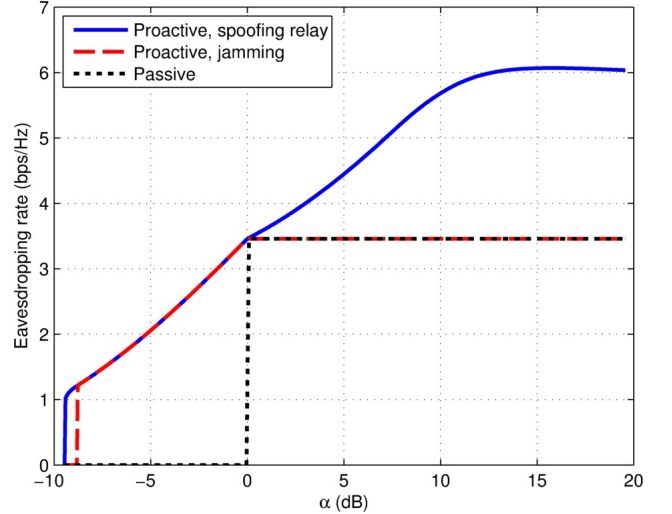


Fig. 4: Eavesdropping rate versus $\alpha \triangleq \|\mathbf{h}_{SE}\|^2 / |h_{SD}|^2$, where $\gamma_0 \triangleq P_S |h_{SD}|^2 / \sigma^2 = 10$ dB and $P_E = P_S$.

to be equipped at **E**, instead of M as for the uniform power splitting scheme.

IV. NUMERICAL RESULTS

In this section, numerical results are provided to evaluate the performance of the proposed proactive eavesdropping via spoofing relay technique. We assume that the suspicious source **S** and the suspicious destination **D** are separated by a fixed distance $d_{SD} = 1000$ meters (m). The legitimate monitor **E** is located on the same line connecting **S** to **D**, with the distance between **S** and **E** denoted as d_{SE} that varies between 100m and 3000m for different eavesdropper locations. Such a setup could correspond to the macro-cell users (with typical cell radius on the order of km). Thus, the distance between **E** and **D** can be expressed as $d_{ED} = |d_{SD} - d_{SE}|$. We assume

that uniform linear arrays with adjacent elements separated by half-wavelength are equipped at the transmitter and receiver of **E**. Furthermore, we assume that all links are dominated by the line-of-sight (LoS) channels that follow the free-space path loss model. Unless otherwise specified, the number of transmitting and receiving antennas at **E** are $N = 2$ and $M = 1$, respectively. The operating frequency is assumed to be 1.8 GHz. We define $\alpha \triangleq \|\mathbf{h}_{SE}\|^2/\|\mathbf{h}_{SD}\|^2$ as the channel power ratio between the eavesdropping and the suspicious links, where all the channels including \mathbf{h}_{SE} and \mathbf{h}_{SD} are generated based on the eavesdropper's location and the LoS path loss model. Furthermore, denote $\gamma_0 \triangleq P_S\|\mathbf{h}_{SD}\|^2/\sigma^2$ as the reference SNR received at **D** with source transmission power P_S and receiver noise power σ^2 . We consider two benchmark schemes, namely passive eavesdropping as discussed in Section II-A, and proactive eavesdropping with jamming only [1], [2]. Note that with the definition given in (3), passive eavesdropping has positive eavesdropping rate only when **E** has better channel than **D** from the suspicious source **S**, i.e., $\alpha \geq 1$. On the other hand, jamming is helpful for enhancing the eavesdropping rate only when **E** has weaker channel than **D**, i.e., $\alpha < 1$.

First, we study the effect of α on the maximum eavesdropping rate achievable by the legitimate monitor with the three eavesdropping schemes. To this end, we assume that the legitimate monitor **E** moves towards **S** from the location with $d_{SE} = 3000\text{m}$ to that with $d_{SE} = 100\text{m}$. Correspondingly, the channel power ratio α increases from around -10dB to 20dB . The transmission power P_S by **S** is fixed to a value such that the reference SNR $\gamma_0 = 10\text{ dB}$, and the maximum transmission power at **E** is set as $P_E = P_S$. The eavesdropping rates R_{ev} versus α with the three schemes are compared in Fig. 4. It is observed that when **E** has a better channel than **D**, i.e., $\alpha > 1$ (0 dB), both passive eavesdropping and jamming-based eavesdropping (with zero jamming power in this case) achieve a constant R_{ev} , which is equal to the channel capacity of the suspicious link from **S** to **D**. In contrast, the proposed proactive eavesdropping scheme with spoofing relaying achieves a significantly higher eavesdropping rate, since it is able to spoof the suspicious source **S** to increase its transmission rate by constructively forwarding the source signal to **D**, which is not possible in the two benchmark schemes. When **E** has a worse channel than **D**, i.e., $\alpha < 1$ (0 dB), the eavesdropping rate with the passive scheme drops to zero, since **E** cannot reliably decode the information sent from **S**. In contrast, as long as α is not too small, the two proactive schemes can achieve strictly positive eavesdropping rate, since they both jam the suspicious link to spoof the source **S** to decrease its transmission rate to be decodable at **E**. Note that in this regime, the proposed spoofing relay technique degenerates to jamming (Case 2 as described in Section III-C), thus the two proactive schemes obtain identical rate performance. As α further decreases, e.g., $\alpha = -10\text{ dB}$, **E** is unable to decode the information sent by **S** even with the two proactive schemes, and thus the eavesdropping rate drops to zero. However, it is worth noting that at around $\alpha = -9\text{dB}$, the proposed spoofing relay technique still achieves strictly positive eavesdropping rate, whereas that with jamming only is zero. This corresponds

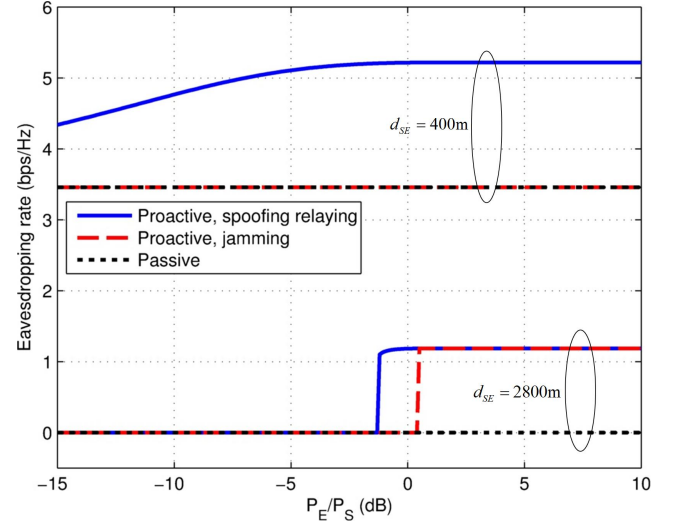


Fig. 5: Eavesdropping rate versus the legitimate monitor's power budget P_E , where $\gamma_0 = 10\text{ dB}$.

to Case 3 as described in Section III-C, where both jamming and destructive information forwarding can be jointly applied to further degrade the suspicious link SNR for **E** to decode the information sent by **S**.

Next, we investigate the effect of the legitimate monitor's power budget P_E on the maximum achievable eavesdropping rate with the three considered schemes. We compare two setups with $d_{SE} = 400\text{m}$ and $d_{SE} = 2800\text{m}$, respectively. The transmission power P_S by **S** is fixed such that $\gamma_0 = 10\text{ dB}$, whereas the power budget P_E at the legitimate monitor varies such that the power ratio P_E/P_S increases from -15 dB to 10 dB . Fig. 5 shows the maximum eavesdropping rate versus P_E/P_S by the three eavesdropping schemes under the two setups. It is first observed that the eavesdropping rate by the passive scheme is independent of P_E , since no transmission is performed at **E**. Furthermore, for the case with $d_{SE} = 400\text{m}$, the eavesdropping rate by the jamming scheme is also independent of P_E , since no jamming is needed when the eavesdropping link is stronger than the suspicious link. In contrast, the eavesdropping rate with the proposed spoofing relay technique under $d_{SE} = 400\text{m}$ firstly increases with P_E , and then approaches to a constant value as P_E gets sufficiently large, which is in accordance with Lemma 1. For the case of $d_{SE} = 2800\text{m}$ where **E** has worse channel than **D**, both the two proactive schemes have zero eavesdropping rate when P_E is sufficiently small, whereas the rate increases to a positive value when P_E exceeds certain thresholds. It is noted that if the eavesdropping link is stronger than the suspicious link (e.g., $d_{SE} = 400\text{m}$), then the proposed scheme always outperforms the jamming-based scheme, regardless of the power budget P_E at the relay. On the other hand, for $d_{SE} = 2800\text{m}$ so that the eavesdropping link is weaker than the suspicious link, an excessive relay power about 2 dB is required by jamming than the proposed scheme in order to achieve the same eavesdropping rate of around 1.2 bps/Hz.

For the proposed spoofing relaying scheme, Fig. 6 plots the optimal power splitting ratio ρ^* at **E** versus P_E/P_S . It

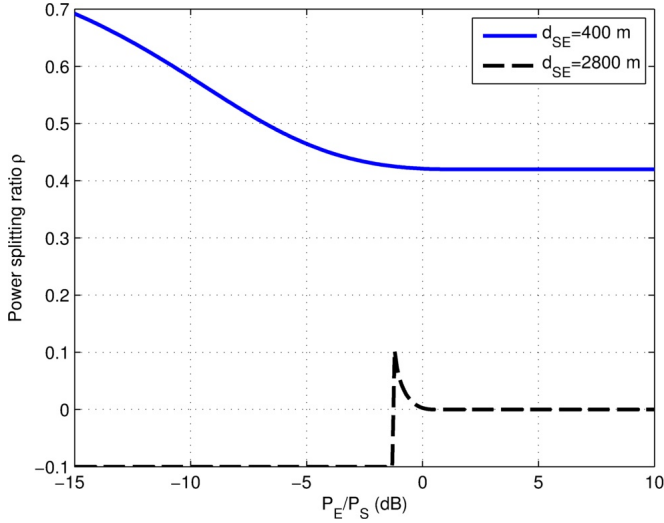


Fig. 6: Optimal power splitting ratio for the proposed spoofing relaying versus P_E , where $\gamma_0 = 10$ dB.

is observed that for the case of $d_{SE} = 400$ m, ρ^* firstly decreases with P_E , since larger transmission power at **E** requires less signal power to be split for information relaying, and hence more power can be split for eavesdropping. As P_E gets sufficiently large, ρ^* approaches to a constant value of 0.42, which is in accordance with that predicted by Lemma 1. On the other hand, for the case of $d_{SE} = 2800$ m, problem (P1) is infeasible when P_E is too small, which is indicated by the infeasible $\rho = -0.1$ in Fig. 6. For P_E/P_S between -2 dB and 0 dB, a small fraction of the signal power received at **E** is split for destructive information forwarding. As P_E/P_S increases to 0 dB, ρ^* becomes zero since jamming alone is optimal in this case, which is consistent with the results in Fig. 5.

Next, we investigate the effect of source transmission power P_S on the eavesdropping rate. Similar to that in Fig. 5 and Fig. 6, we consider two setups with $d_{SE} = 400$ m and $d_{SE} = 2800$ m, respectively. The power budget P_E at **E** is fixed such that $P_E|h_{SD}|^2/\sigma^2 = 10$ dB, whereas the transmission power P_S by the suspicious source varies such that the reference SNR γ_0 increases from 0 dB to 20 dB. Fig. 7 shows the maximum achievable eavesdropping rate by the three considered schemes versus γ_0 under each of the two setups. It is first observed that for the case of $d_{SE} = 400$ m where **E** has better channel than **D**, the eavesdropping rate with all three considered schemes increases with P_S . However, the proposed spoofing relaying scheme performs significantly better than the other two schemes, due to the constructive relaying performed at **E** that enhances the effective channel capacity from **S** to **D**. For the case of $d_{SE} = 2800$ m, the eavesdropping rate by both passive eavesdropping and jamming only is zero due to the poor channel between **S** and **E**. In contrast, the proposed spoofing relaying technique is able to achieve strictly positive eavesdropping rate for γ_0 below a certain threshold, beyond which the eavesdropping rate drops to zero since the suspicious transmission rate cannot be degraded to a value decodable by **E** with its given transmit power constraint P_E .

Lastly, by assuming equal number transmitting and receiving antennas at the eavesdropper, i.e., $M = N \triangleq \bar{N}$, Fig. 8

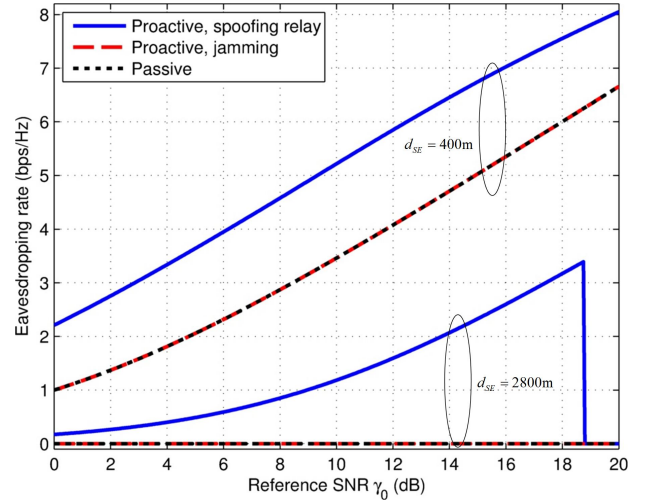


Fig. 7: Eavesdropping rate versus $\gamma_0 \triangleq P_S|h_{SD}|^2/\sigma^2$.

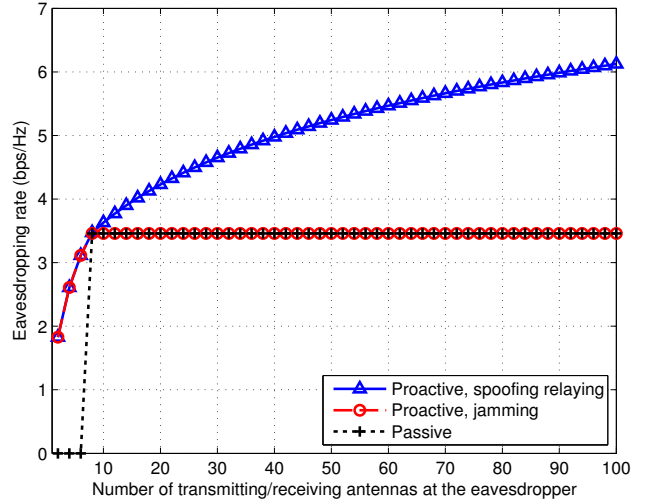


Fig. 8: Eavesdropping rate versus the number of transmitting/receiving antennas at the eavesdropper.

shows the eavesdropping rate versus \bar{N} for $d_{SE} = 2800$ m, $\gamma_0 = 10$ dB, and $P_E = P_S$. Note that since the loop channel \mathbf{H}_{EE} is of rank-1 under the LoS assumption, the ZF constraint (5) is feasible as long as $N \geq 2$. Fig. 8 shows that the performance of all the three eavesdropping schemes in general improves with the increasing of \bar{N} , which is expected due to the more powerful receiving/transmitting beamforming gains as more antennas are used. However, for the two benchmark schemes, no further improvement on the eavesdropping rate is possible for \bar{N} beyond 6, since the eavesdropping rate is fundamentally limited by the source transmission rate, which neither passive eavesdropping nor jamming is able to improve when the eavesdropping link becomes better than the suspicious link. In contrast, thanks to the constructive relaying, the proposed spoofing relaying technique is able to achieve continuous eavesdropping rate improvement as \bar{N} increases, though with a diminishing gain. This again shows the superior performance of the proposed eavesdropping strategy over the two benchmark schemes.

V. CONCLUSIONS

This paper has studied the new wireless information surveillance problem in the general paradigm of wireless security. A novel proactive eavesdropping scheme with spoofing relaying technique has been proposed. With the proposed scheme, the legitimate monitor acts as a full-duplex relay for simultaneous eavesdropping and spoofing relaying to render the suspicious source to vary transmission rate in favor of the eavesdropping performance. The receive power splitting ratios and the transmit precoding matrix at the legitimate monitor are jointly optimized for eavesdropping rate maximization. Numerical results show that the proposed spoofing relay technique significantly enhances the information surveillance performance as compared to the two benchmark schemes with passive or jamming-based eavesdropping.

APPENDIX A PROOF OF THEOREM 1

To show Theorem 1, we first apply the triangle inequality to (17), which yields

$$\tilde{\gamma}_D(\rho, \mathbf{W}) \leq \frac{(|h_{SD}| + |\hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}|)^2 \tilde{P}_S}{1 + \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}\|^2}, \quad \forall \mathbf{W}, \quad (36)$$

where equality holds if and only if \mathbf{W} is chosen such that the two effective signal paths from \mathbf{S} to \mathbf{D} add constructively, i.e., $\angle h_{SD} = \angle \hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}$. Furthermore, since an arbitrary phase shifting of \mathbf{W} does not alter the feasibility of the power constraint in (19), problem (19) is thus equivalent to

$$\tilde{\gamma}_D^{\max}(\rho) \triangleq \begin{cases} \max_{\mathbf{W}} & \tilde{\gamma}_D(\mathbf{W}) \triangleq \frac{(|h_{SD}| + |\hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}|)^2 \tilde{P}_S}{1 + \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}\|^2} \\ \text{s.t.} & \tilde{P}_S \|\mathbf{W} \hat{\mathbf{h}}_{SE}\|^2 + \|\mathbf{W}\|_F^2 \leq \tilde{P}_E. \end{cases} \quad (37)$$

Lemma 2. *The optimal solution to problem (37) is*

$$\mathbf{W}^* = \sqrt{\mu^*} \tilde{\mathbf{h}}_{ED} \tilde{\mathbf{h}}_{SE}^H, \quad (38)$$

where μ^* is the optimal solution to the following optimization problem

$$\tilde{\gamma}_D^{\max}(\rho) \triangleq \begin{cases} \max_{\mu} & \tilde{\gamma}_D(\mu) \triangleq \frac{(|h_{SD}| + \sqrt{\mu} \|\hat{\mathbf{h}}_{ED}\| \|\hat{\mathbf{h}}_{SE}\|)^2 \tilde{P}_S}{1 + \mu \|\hat{\mathbf{h}}_{ED}\|^2} \\ \text{s.t.} & 0 \leq \mu \leq \frac{\tilde{P}_E}{\tilde{P}_S \|\hat{\mathbf{h}}_{SE}\|^2 + 1}. \end{cases} \quad (39)$$

Proof: We show Lemma 2 by construction. Suppose that an optimal solution to (37) is given by $\mathbf{W}' = \sqrt{\mu'} \tilde{\mathbf{W}}$, with $\|\tilde{\mathbf{W}}\|_F = 1$, and the resulting optimal value is $\tilde{\gamma}_D(\mathbf{W}')$. We then construct an alternative solution \mathbf{W}'' in the form of (38), i.e., $\mathbf{W}'' = \sqrt{\mu''} \tilde{\mathbf{h}}_{ED} \tilde{\mathbf{h}}_{SE}^H$, with

$$\mu'' = \mu' \frac{|\hat{\mathbf{h}}_{ED}^H \tilde{\mathbf{W}} \hat{\mathbf{h}}_{SE}|^2}{\|\hat{\mathbf{h}}_{ED}\|^2 \|\hat{\mathbf{h}}_{SE}\|^2} \leq \mu', \quad (40)$$

where the last inequality follows from the sub-multiplicativity property of the Frobenius norm, i.e., $\|\mathbf{AB}\|_F \leq \|\mathbf{A}\|_F \|\mathbf{B}\|_F$ for any conformable matrices (vectors) \mathbf{A} and \mathbf{B} [29]. We aim to show that the newly constructed matrix \mathbf{W}'' is feasible to

problem (37), and also returns an objective value no smaller than $\tilde{\gamma}_D(\mathbf{W}')$. To this end, we first show the following:

$$\tilde{P}_S \|\mathbf{W}'' \hat{\mathbf{h}}_{SE}\|^2 + \|\mathbf{W}''\|_F^2 = \tilde{P}_S \mu' \frac{|\hat{\mathbf{h}}_{ED}^H \tilde{\mathbf{W}} \hat{\mathbf{h}}_{SE}|^2}{\|\hat{\mathbf{h}}_{ED}\|^2} + \mu'' \quad (41)$$

$$\leq \tilde{P}_S \mu' \|\tilde{\mathbf{W}} \hat{\mathbf{h}}_{SE}\|^2 + \mu' \quad (42)$$

$$\leq \tilde{P}_E, \quad (43)$$

where (42) follows from $\mu'' \leq \mu'$ and the Cauchy-Schwarz inequality $|\mathbf{a}^H \mathbf{b}|^2 \leq \|\mathbf{a}\|^2 \|\mathbf{b}\|^2$, $\forall \mathbf{a}, \mathbf{b}$; and (43) is true since $\mathbf{W}' = \sqrt{\mu'} \tilde{\mathbf{W}}$ must satisfy the power constraint of problem (37). The above result shows that the newly constructed matrix \mathbf{W}'' also satisfies the power constraint at \mathbf{E} , and hence is feasible to problem (37). Furthermore, the following results can be obtained,

$$\begin{aligned} |\hat{\mathbf{h}}_{ED}^H \mathbf{W}'' \hat{\mathbf{h}}_{SE}| &= \sqrt{\mu''} \|\hat{\mathbf{h}}_{ED}\| \|\hat{\mathbf{h}}_{SE}\| = \sqrt{\mu'} |\hat{\mathbf{h}}_{ED}^H \tilde{\mathbf{W}} \hat{\mathbf{h}}_{SE}| \\ &= |\hat{\mathbf{h}}_{ED}^H \mathbf{W}' \hat{\mathbf{h}}_{SE}|, \end{aligned} \quad (44)$$

$$\begin{aligned} \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}''\| &= \sqrt{\mu''} \|\hat{\mathbf{h}}_{ED}\| = \sqrt{\mu'} \frac{|\hat{\mathbf{h}}_{ED}^H \tilde{\mathbf{W}} \hat{\mathbf{h}}_{SE}|}{\|\hat{\mathbf{h}}_{SE}\|} \\ &\leq \sqrt{\mu'} \|\hat{\mathbf{h}}_{ED}^H \tilde{\mathbf{W}}\| = \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}'\|. \end{aligned} \quad (45)$$

Based on (44) and (45), it is not difficult to conclude that $\tilde{\gamma}_D(\mathbf{W}'') \geq \tilde{\gamma}_D(\mathbf{W}')$. In summary, for any optimal solution \mathbf{W}' to problem (37), we can always construct a feasible solution \mathbf{W}'' in the form of (38) that achieves no smaller objective value; thus, \mathbf{W}'' must also be optimal. Furthermore, problem (39) is resulted by substituting (38) into (37). This completes the proof of Lemma 2. ■

The uni-variate optimization problem (39) can be then solved by examining its first-order derivative. Together with Lemma 2, the results in Theorem 1 can be obtained. This completes the proof of Theorem 1.

APPENDIX B PROOF OF THEOREM 2

To show Theorem 2, we first apply the triangle inequality to (17), which yields

$$\tilde{\gamma}_D(\rho, \mathbf{W}) \geq \frac{(|h_{SD}| - |\hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}|)^2 \tilde{P}_S}{(1 + \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}\|^2) \sigma^2}, \quad \forall \mathbf{W}, \quad (46)$$

where equality holds if and only if \mathbf{W} is chosen such that the two effective signal paths from \mathbf{S} to \mathbf{D} add destructively, i.e., $\angle h_{SD} = \pi + \angle \hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}$. Furthermore, since an arbitrary phase shifting of \mathbf{W} does not alter the feasibility of problem (22), the optimal solution to (22) can be obtained by solving

$$\tilde{\gamma}_D^{\min}(\rho) \triangleq \begin{cases} \min_{\mathbf{W}} & \tilde{\gamma}_D(\mathbf{W}) \triangleq \frac{(|h_{SD}| - |\hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}|)^2 \tilde{P}_S}{1 + \|\hat{\mathbf{h}}_{ED}^H \mathbf{W}\|^2} \\ \text{s.t.} & \tilde{P}_S \|\mathbf{W} \hat{\mathbf{h}}_{SE}\|^2 + \|\mathbf{W}\|_F^2 \leq \tilde{P}_E. \end{cases} \quad (47)$$

Next, we derive the optimal structure of the solution to (47). Recall that \mathbf{W} is a matrix of dimension $r_0 \times M$. Define an r_0 -dimensional unitary matrix $\mathbf{U} \triangleq [\tilde{\mathbf{h}}_{ED} \ \mathbf{U}_{\perp}]$, where $\mathbf{U}_{\perp} \in \mathbb{C}^{r_0 \times (r_0-1)}$ is the orthogonal complement of $\tilde{\mathbf{h}}_{ED}$ such

that $\mathbf{U}^H \mathbf{U} = \mathbf{I}_{r_0}$. Similarly, define an M -dimensional unitary matrix $\mathbf{V} \triangleq [\tilde{\mathbf{h}}_{SE} \ \mathbf{V}_\perp]$, where $\mathbf{V}^H \mathbf{V} = \mathbf{I}_M$. Then any matrix $\mathbf{W} \in \mathbb{C}^{r_0 \times M}$ can be expressed as

$$\mathbf{W} = \mathbf{U} \mathbf{Q} \mathbf{V}^H = [\tilde{\mathbf{h}}_{ED} \ \mathbf{U}_\perp] \begin{bmatrix} q_{11} & \mathbf{q}_{12}^H \\ \mathbf{q}_{21} & \mathbf{Q}_{22} \end{bmatrix} \begin{bmatrix} \tilde{\mathbf{h}}_{SE}^H \\ \mathbf{V}_\perp^H \end{bmatrix}, \quad (48)$$

where $q_{11} \in \mathbb{C}$, $\mathbf{q}_{12} \in \mathbb{C}^{(M-1) \times 1}$, $\mathbf{q}_{21} \in \mathbb{C}^{(r_0-1) \times 1}$, and $\mathbf{Q}_{22} \in \mathbb{C}^{(r_0-1) \times (M-1)}$ are the new optimization variables after unitary transformations by \mathbf{U} and \mathbf{V} . By substituting \mathbf{W} with (48), we have the following results:

$$|\hat{\mathbf{h}}_{ED}^H \mathbf{W} \hat{\mathbf{h}}_{SE}| = |q_{11}| \|\hat{\mathbf{h}}_{ED}\| \|\hat{\mathbf{h}}_{SE}\| \quad (49)$$

$$\|\tilde{\mathbf{h}}_{ED}^H \mathbf{W}\|^2 = \|\hat{\mathbf{h}}_{ED}\|^2 (|q_{11}|^2 + \|\mathbf{q}_{12}\|^2) \quad (50)$$

$$\|\mathbf{W} \hat{\mathbf{h}}_{SE}\|^2 = \|\hat{\mathbf{h}}_{SE}\|^2 (|q_{11}|^2 + \|\mathbf{q}_{21}\|^2) \quad (51)$$

$$\|\mathbf{W}\|_F^2 = |q_{11}|^2 + \|\mathbf{q}_{21}\|^2 + \|\mathbf{q}_{12}\|^2 + \|\mathbf{Q}_{22}\|_F^2. \quad (52)$$

It is observed from (49)-(52) that the objective value of problem (47) is independent of \mathbf{q}_{21} and \mathbf{Q}_{22} . Besides, the left hand side (LHS) of the power constraint in problem (47) increases with $\|\mathbf{q}_{21}\|^2$ and $\|\mathbf{Q}_{22}\|_F^2$. Thus, without loss of optimality, we can set $\mathbf{q}_{21} = \mathbf{0}$ and $\mathbf{Q}_{22} = \mathbf{0}$. Furthermore, as both the objective value and the transmit power depend on \mathbf{q}_{12} via its norm $\|\mathbf{q}_{12}\|$ only, we can assume without loss of optimality that $\mathbf{q}_{12} = \sqrt{z_2} [1 \ 0 \cdots 0]^T$ for $z_2 \geq 0$. Similarly, we may assume $q_{11} = \sqrt{z_1}$ for $z_1 \geq 0$ without loss of optimality. Therefore, it follows from (48) that the optimal solution to (47) can be expressed as

$$\mathbf{W} = \tilde{\mathbf{h}}_{ED} \left(\sqrt{z_1} \tilde{\mathbf{h}}_{SE} + \sqrt{z_2} \tilde{\mathbf{h}}_{SE}^\perp \right)^H. \quad (53)$$

By substituting (53) into problem (47), we obtain the optimization problem (24) for determining the optimal weighting coefficients z_1 and z_2 .

This completes the proof of Theorem 2.

APPENDIX C PROOF OF THEOREM 3

Note that the objective value of problem (24) is always non-negative, and it equals to zero if $z_1 = |h_{SD}|^2 / (\|\tilde{\mathbf{h}}_{ED}\|^2 \|\tilde{\mathbf{h}}_{SE}\|^2) \triangleq z_1'$. Thus, if z_1' is achievable, i.e., $z_1' \leq \tilde{P}_E / (1 + \tilde{P}_S \|\tilde{\mathbf{h}}_{SE}\|^2)$, the pair $(z_1', 0)$ is obviously the optimal solution to (24). This corresponds to the first case of (25). For the remaining cases, it can be verified that at the optimal solution, the power constraint of (24) should be satisfied with equality, since otherwise, one can always increase z_2 to further minimize the objective value. Therefore, the variable z_2 can be eliminated by substituting with z_1 , and the problem reduces an uni-variate optimization problem, which can be solved by examining its first-order derivative. The details are omitted for brevity.

APPENDIX D PROOF OF THEOREM 4

The key for proving Theorem 4 is to use the fact that all the three functions $\tilde{\gamma}_E(\boldsymbol{\rho})$, $\tilde{\gamma}_D^{\max}(\boldsymbol{\rho})$, and $\tilde{\gamma}_D^{\min}(\boldsymbol{\rho})$ depend on $\boldsymbol{\rho}$ only via the term $\|\mathbf{h}_{SE}(\boldsymbol{\rho})\|^2 = \mathbf{h}_{SE}^H \text{diag}(\boldsymbol{\rho}) \mathbf{h}_{SE} = \sum_{m=1}^M \rho_m |h_{SE,m}|^2$, where $h_{SE,m}$ denotes the m th element

of \mathbf{h}_{SE} . Assume that $(\boldsymbol{\rho}', \tilde{\gamma}_D')$ is an optimal solution to (P3), with the m th element of $\boldsymbol{\rho}'$ given by $0 \leq \rho'_m \leq 1$, $m = 1, \dots, M$. We construct a new power splitting vector $\boldsymbol{\rho}'' = \rho'' \mathbf{1}$, with $\rho'' = \left(\sum_{m=1}^M \rho'_m |h_{SE,m}|^2 \right) / \left(\sum_{m=1}^M |h_{SE,m}|^2 \right)$. It is obvious that $0 \leq \rho'' \leq 1$, and thus the constraint $\mathbf{0} \preceq \boldsymbol{\rho}'' \preceq \mathbf{1}$ is satisfied. Furthermore, we also have $\|\hat{\mathbf{h}}_{SE}(\boldsymbol{\rho}'')\|^2 = \|\hat{\mathbf{h}}_{SE}(\boldsymbol{\rho}')\|^2$, and hence $\tilde{\gamma}_E(\boldsymbol{\rho}'') = \tilde{\gamma}_E(\boldsymbol{\rho}')$, $\tilde{\gamma}_D^{\max}(\boldsymbol{\rho}'') = \tilde{\gamma}_D^{\max}(\boldsymbol{\rho}')$, and $\tilde{\gamma}_D^{\min}(\boldsymbol{\rho}'') = \tilde{\gamma}_D^{\min}(\boldsymbol{\rho}')$. Therefore, the pair $(\boldsymbol{\rho}'', \tilde{\gamma}_D')$ is also an optimal solution to (P3). This completes the proof of Theorem 4.

APPENDIX E PROOF OF THEOREM 5

The proof of Theorem 5 is similar to that of Theorem 4, which exploits the fact that the power splitting vector $\boldsymbol{\rho}$ affects the SNRs at both \mathbf{D} and \mathbf{E} only via the term $\|\hat{\mathbf{h}}_{SE}(\boldsymbol{\rho})\|^2 = \sum_{m=1}^M \rho_m |h_{SE,m}|^2$. Let $\boldsymbol{\rho}_{\text{ups}}^* = \rho_{\text{ups}}^* \mathbf{1}$ be the optimal UPS vector to problem (P3). If $\rho_{\text{ups}}^* = 0$ or $\rho_{\text{ups}}^* = 1$, then Theorem 5 is already satisfied. Thus, we assume $0 < \rho_{\text{ups}}^* < 1$. In this case, it can be verified that there always exists an integer $m' \in \{1, \dots, M\}$ such that both the following inequalities hold,

$$\sum_{m=1}^{m'-1} |h_{SE,[m]}|^2 < \rho_{\text{ups}}^* \sum_{m=1}^M |h_{SE,m}|^2, \quad (54)$$

$$\sum_{m=1}^{m'} |h_{SE,[m]}|^2 \geq \rho_{\text{ups}}^* \sum_{m=1}^M |h_{SE,m}|^2, \quad (55)$$

where $[\cdot]$ is the permutation operation such that $|h_{SE,[1]}|^2 \geq \cdots \geq |h_{SE,[M]}|^2$. As a result, we define a new power splitting vector $\boldsymbol{\rho}_{\text{bps}}$ with binary power splitting (BPS) over $M-1$ receiving antennas such that

$$\rho_{\text{bps},m} = \begin{cases} 1, & m = [1], \dots, [m'-1], \\ \rho_{\text{bps}}, & m = [m'], \\ 0, & m = [m'+1], \dots, [M], \end{cases} \quad (56)$$

where

$$\rho_{\text{bps}} = \frac{\rho_{\text{ups}}^* \sum_{m=1}^M |h_{SE,m}|^2 - \sum_{m=1}^{m'-1} |h_{SE,[m]}|^2}{|h_{SE,[m']}|^2}. \quad (57)$$

It can be verified that $0 < \rho_{\text{bps}} \leq 1$, and hence $\mathbf{0} \preceq \boldsymbol{\rho}_{\text{bps}} \preceq \mathbf{1}$ is satisfied. Furthermore, we have $\|\hat{\mathbf{h}}_{SE}(\boldsymbol{\rho}_{\text{bps}})\|^2 = \|\hat{\mathbf{h}}_{SE}(\boldsymbol{\rho}_{\text{ups}}^*)\|^2$. Thus, $\boldsymbol{\rho}_{\text{bps}}$ must also be an optimal solution to problem (P3). This completes the proof of Theorem 5.

REFERENCES

- [1] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Letters*, vol. 5, no. 1, pp. 80–83, Feb. 2016.
- [2] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," submitted to *IEEE Trans. Wireless Commun.*, [Online] Available: <http://arxiv.org/abs/1512.02754>.
- [3] Y. Liang, H. V. Poor, and S. Shamai, *Information theoretic security*, Foundations and Trends in Communications and Information Theory, 2009.
- [4] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.
- [5] A. D. Wyner, "The wire-tap channel," *Bell Sys. Techn. Journ.*, vol. 54, no. 8, pp. 1355–1387, 1975.

- [6] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [8] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Aug. 2013.
- [9] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.
- [10] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4757–4767, Nov. 2013.
- [11] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.
- [12] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.
- [13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [14] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. Inf. Theory Workshop*, pp. 87–89, Sept. 2001.
- [15] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
- [16] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wiretapper," in *Proc. Inf. Theory Workshop*, pp. 595–600, Sept. 2007.
- [17] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sept. 2011.
- [18] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sept. 2013.
- [19] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
- [20] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: construction and countermeasures," in *Proc. IEEE Asilomar Conference on Signals, Systems and Computers*, pp. 265–269, Nov. 2011.
- [21] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, June 2015.
- [22] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE PIMRC*, Sept. 2013, pp. 13–18.
- [23] A. A. Kapetanovic, D. Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive MIMO," in *Proc. IEEE PIMRC*, Sept. 2014, pp. 585–589.
- [24] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.
- [25] J.-M. Kang, C. In, and H.-M. Kim, "Detection of pilot contamination attack for multi-antenna based secrecy systems," in *Proc. IEEE VTC Spring*, May 2015, pp. 1–5.
- [26] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, July 2015.
- [27] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.
- [28] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept. 2014.
- [29] R. A. Horn and C. R. Johnson, *Matrix Analysis*, New York: Cambridge Univ. Press, 2nd edition, 2013.